We claim:

1. A method comprising:

    detecting a power line activity pattern on a power line;

    determining whether the power line activity pattern is unacceptable; and,

5   upon determining that the power line activity pattern is unacceptable, performing a

    predetermined action.

2. The method of claim 1, wherein determining whether the power line activity pattern

    is unacceptable comprises testing the power line activity pattern against a database of

    unacceptable power line activity patterns.

10 3. The method of claim 1, wherein determining whether the power line activity pattern

    is unacceptable comprises testing the power line activity pattern against a model of

    acceptable power line activity.

4. The method of claim 1, wherein performing a predetermined action comprises

    alerting a user.

15 5. The method of claim 1, wherein performing a predetermined action comprises

    generating an event.

6. The method of claim 1, wherein the method is performed by execution of a computer

    program stored on a machine-readable medium by a processor.

7. A power line monitoring system comprising:

a power line monitoring daemon to detect a power line activity pattern and test the pattern for unacceptability; and,

a database of unacceptable power line activity patterns against which the power line

5 monitoring daemon tests the pattern for unacceptability, the daemon performing an action in response to the pattern being unacceptable.

8. The system of claim 7, further comprising:

a log file to which the daemon logs the power line activity pattern detected; and,

an analysis tool to enhance the database based on the power line activity pattern

10 detected.

9. A power line monitoring system comprising:

a power line monitoring daemon to detect a power line activity pattern and test the pattern for unacceptability; and,

a model of acceptable power line activity behavior against which the power line

15 monitoring daemon tests the pattern for unacceptability, the daemon performing an action in response to the pattern being unacceptable.

10. The system of claim 9, further comprising:

a log file to which the daemon logs the power line activity pattern detected; and,

an analysis tool to enhance the model based on the power line activity pattern

20 detected.

11. An architecture for an automation system, the automation system to control and monitor a plurality of devices, the architecture comprising:

at least one look-up service to maintain at least one database of the plurality of devices by a plurality of device attributes including device type and physical location, and of a plurality of device objects corresponding to the plurality of devices by mapping a name for each device object to at least one address for each device object;

a soft-state store to manage at least periodic refresh information for the plurality of devices and the plurality of device objects, the refresh information managed by the soft-state store as a plurality of soft-state variables;

a publication/subscription eventing component to enable subscriptions to events related to changes in the plurality of soft-state variables managed by the soft-state store; and,

a power line monitoring daemon to detect problems with the plurality of devices that are power line devices.

12. The architecture of claim 11, wherein the power line monitoring daemon uses pattern-based detection for detecting unacceptable power line activity.

13. The architecture of claim 12, wherein the power line monitoring daemon matches power line patterns against unacceptable power line patterns stored in a pattern database.

14. The architecture of claim 11, wherein the power line monitoring daemon uses model-based detection for detecting acceptable power line activity.

15. The architecture of claim 14, wherein the power line monitoring daemon tests power line patterns against a pattern model of acceptable power line patterns.